it difficult to retain or quickly retrieve such additional data. Other cardholders simply are unhappy with the slow and tedious experience of (sometimes repeatedly) providing additional data. Still others may not wish to share additional data due to trustworthiness concerns. Cardholders tend to terminate transactions because the attendant security measures are overly cumbersome or undesirable. Accordingly, increased security measures reduce the proportion of successful financial transactions, leading to losses for merchants, banks, and other financial entities. Moreover, certain security measures may not operate properly on particular platforms (e.g., a mobile device) leading to further cardholder frustration and resulting in termination of the transaction.

BRIEF SUMMARY OF THE DISCLOSURE

In one aspect, a method for monitoring execution of a digital authentication program is provided. The method is implemented using an authentication monitoring (AM) computer device comprising a processor and a memory device, the method comprising: receiving an authentication data file from an authenticating computer device executing the digital authentication program, wherein the authenticating computer device is associated with an authenticating entity, and wherein the digital authentication program includes one or more authentication rules; extracting at least one authentication value from the authentication data file; determining that the authentication value fails to comply with the one or more authentication rules; updating a stored metric associated with the authentication value for the authenticating computer device; determining, based on the testing, that the stored metric fails to meet a predefined benchmark for the stored metric; and initiating an authentication remediation process, wherein the authentication remediation process causes an update to the digital authentication program used by the authenticating computer device.

In another aspect, a system for monitoring an execution of a digital authentication program is provided. The system includes an authentication monitoring (AM) computer device comprising a processor and a memory device, the AM computer device configured to: receive an authentication data file from an authenticating computer device executing the digital authentication program, wherein the authenticating computer device is associated with an authenticating entity, and wherein the digital authentication program includes one or more authentication rules;

extract at least one authentication value from the authentication data file; determine that the authentication value fails to comply with the one or more authentication rules; update a stored metric associated with the authentication value for the authenticating computer device; determine, based on the testing, that the stored metric fails to meet a predefined benchmark for the stored metric; and initiate an authentication remediation process, wherein the authentication remediation process causes an update to the digital authentication program used by the authenticating computer device.

In yet another aspect, a non-transitory computer readable medium that includes computer executable instructions for monitoring an execution of a digital authentication program is provided. When executed by an authentication monitoring (AM) computer device comprising a processor and a memory device, the computer executable instructions cause the AM computer device to: receive an authentication data file from an authenticating computer device executing the digital authentication program, wherein the authenticating computer device is associated with an authenticating entity, and wherein the digital authentication program includes one or more authentication rules; extract at least one authentication value from the authentication data file; determine that the authentication value fails to comply with the one or more authentication rules; update a stored metric associated with the authentication value for the authenticating computer device; determine, based on the testing, that the stored metric fails to meet a predefined benchmark for the stored metric; and initiate an authentication remediation process, wherein the authentication remediation process causes an update to the digital authentication program used by the authenticating computer device.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram illustrating a multi-party transaction card system for enabling transactions that involve digital authentication programs.